ROYAUME DE BELGIQUE

COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

Bruxelles, le

Adresse : Rue Haute, 139, B-1000 Bruxelles
Tél.: +32(0)2/213.85.40 E-mail : commission@privacy.fgov.be
Fax.: +32(0)2/213.85.65 http://www.privacy.fgov.be/

DELIBERATION AF N° 01 / 2005 du 10 janvier 2005

N. Réf. : SA1 / FO / 2004 / 001

OBJET : Délibération concernant la demande formulée par la Banque Carrefour de la Sécurité sociale afin d'avoir accès aux données d'identification électroniques conservées par FEDICT en vue de la gestion des utilisateurs et de l'accès, ainsi que de la communication du secteur social avec les citoyens et les collaborateurs d'institutions et d'organisations.

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, en particulier les articles 31*bis* et 36*bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée*, en particulier l'article 18 ;

Vu la demande formulée par Banque Carrefour de la Sécurité sociale, reçue le 29 novembre 2004 ;

Vu l'avis juridique et technique du Service public fédéral Technologie de l'Information et de la Communication, reçu le 22 décembre 2004 ;

Vu le rapport du Président ;

Adopte, après délibération, la décision suivante, le 10 janvier 2005:

I. OBJET DE LA DEMANDE

La finalité de la demande est d'autoriser la Banque Carrefour de la Sécurité sociale, les institutions de sécurité sociale, les organismes qui sont ou seront intégrés dans le réseau de la sécurité sociale et les dispensateurs de droits supplémentaires, ci-après les demandeurs, à accéder au fichier d'identification électronique de Fedict dans lequel sont repris les citoyens ainsi que les collaborateurs des institutions et organisations qui se sont inscrites sur le portail fédéral. Les demandeurs désirent obtenir cet accès en vue du développement d'applications électroniques dans le domaine de la gestion des utilisateurs et de l'accès, de manière à éviter des enregistrements faisant double emploi.

II. EXAMEN DE LA DEMANDE

A. LEGISLATION APPLICABLE.

A.1. Article 36bis de la loi du 8 décembre 1992 (LVP).

A.1.1. En vertu de cette disposition, « *toute communication électronique de données à caractère personnel par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe* [du comité sectoriel pour l'autorité fédérale] ».

Les demandeurs souhaitent obtenir la communication électronique de données à caractère personnel mémorisées par Fedict, un service public fédéral.

Par conséquent, le comité sectoriel pour l'autorité fédérale est compétent.

A ce propos, la Commission attire l'attention sur une lacune de la loi. Il n'est pas logique qu'une autorisation soit uniquement prévue pour la communication électronique de données à caractère personnel en provenance d'autorités fédérales et que cette communication puisse avoir lieu sans la moindre autorisation, et donc sans aucun contrôle, lorsqu'il s'agit de données à caractère personnel détenues par les services publics des Communautés et Régions ainsi que par les établissements publics qui en relèvent.

A.1.2. La Commission comprend que pour des considérations d'ordre pratique, la demande n'a pas seulement été formulée pour les organismes faisant déjà partie du réseau de la sécurité sociale mais aussi au nom de ceux qui seront intégrés ultérieurement dans celui-ci.

Il n'est guère efficace qu'à chaque fois qu'un nouvel organisme adhère au réseau de la sécurité sociale, une autorisation distincte doive être demandée en vue de développer une gestion des utilisateurs et de l'accès similaire à celle des autres instances appartenant déjà au réseau de la sécurité sociale. Afin de pouvoir devenir membre du réseau de la sécurité sociale, un organisme doit respecter des règles strictes en matière de sécurité de l'information (voir plus bas, au point D). Le comité sectoriel de la sécurité sociale y veille au demeurant. Ceci veut dire que de tels organismes offriront toujours des garanties suffisantes en ce qui concerne la sécurité.

A la lumière de ce qui précède, la Commission estime que la demande, pour autant qu'elle concerne des instances qui adhéreront ultérieurement au réseau de la sécurité sociale, est également recevable.

A.1.3. La transparence est requise en vue d'un contrôle. Concrètement : il faut que la Commission sache quels organismes auront accès aux données du fichier d'identification de Fedict par suite de cette autorisation. Vu la fonction dirigeante qu'elle remplit au sein du réseau de la sécurité sociale, la Banque Carrefour de la Sécurité sociale est la mieux placée pour renseigner la Commission à ce sujet. La Commission souhaite dès lors que la Banque Carrefour de la Sécurité sociale tienne à sa disposition une liste reprenant l'identité de toutes les institutions de sécurité sociale, de tous les organismes intégrés dans le réseau de la sécurité sociale en vertu de l'article 18 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et des dispensateurs de droits supplémentaires visés à l'article 11bis de la loi précitée qui auront accès au fichier d'identification électronique de Fedict. Cette liste sera mise à jour chaque fois que l'accès sera accordé à un nouvel organisme.

A.2. Article 4 de la loi du 8 décembre 1992 (LVP).

Les données enregistrées dans le fichier d'identification de Fedict sont des données à caractère personnel, dont l'article 4 de la LVP n'autorise le traitement que pour des finalités déterminées, explicites et légitimes. En outre, les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

B. FINALITE.

Entre autres missions, la Banque Carrefour de la Sécurité sociale est chargée, en vertu de l'article 2bis de la loi du 15 janvier 1990, de :

- « *développer une stratégie commune en matière d'e-government dans la sécurité sociale et d'en surveiller le respect* » ;
- « *promouvoir et de veiller à l'homogénéité et à la cohérence de la politique avec cette stratégie commune* » ;
- « *développer les normes, les standards et l'architecture de base nécessaires pour une mise en oeuvre efficace de la technologie de l'information et de la communication à l'appui de cette stratégie et d'en surveiller le respect* » ;
- « *gérer la collaboration avec les autres autorités en matière d'e-government et de technologie de l'information et de la communication* ».

Elle est en outre chargée de « (...) *soutenir les institutions de sécurité sociale afin de leur permettre au moyen des nouvelles technologies d'exécuter d'une manière effective et efficace leurs missions au profit des utilisateurs de leurs services, avec un minimum de charges administratives et de frais pour les intéressés* (...) » (art. 3bis de la loi du 15 janvier 1990).

C'est dans l'intention d'accomplir ces missions légales que la Banque Carrefour de la Sécurité sociale demande l'accès à un certain nombre de données à caractère personnel en possession de Fedict. Plus particulièrement en vue de la concrétisation du « e-government », elle désire pouvoir disposer de ces données afin de développer une gestion des utilisateurs et de l'accès permettant une identification et une authentification de l'utilisateur selon les mêmes modalités pour toutes les applications concernant ce domaine. Des informations personnalisées ou non pourront ainsi être présentées ou expédiées par voie électronique à l'intéressé.

Conséquence de la mission confiée à la Banque Carrefour de la Sécurité sociale : les organismes actifs au sein de la sécurité sociale, et plus particulièrement dans le réseau de la sécurité sociale, opéreront selon un même système dans le cadre du « e-government » et auront donc besoin des mêmes données.

Il ressort de ce qui a été auparavant exposé que la finalité poursuivie est déterminée, explicite et légitime au sens de l'article 4, § 1, 2° de la loi du 8 décembre 1992.

C. PROPORTIONNALITE.

C.1. Par rapport aux données

Les données issues du fichier de Fedict dont les demandeurs désirent faire usage sont :

- le numéro d'identification de la sécurité sociale (pour autant que le demandeur soit autorisé à utiliser celui-ci) ;
- le nom et le prénom ;
- le rôle (citoyen ou collaborateur) ;
- l'adresse électronique ;
- la langue ;
- le nom d'utilisateur.

Si l'intéressé est un collaborateur, il faut encore ajouter les données suivantes :

- le numéro d'entreprise de l'institution ou organisation concernée ;
- le nom de l'institution ou organisation ;
- son adresse officielle ;
- l'état (actif, bloqué ou suspendu).

Le numéro d'identification de la sécurité sociale, le nom, le prénom et le nom d'utilisateur sont indispensables pour pouvoir établir avec certitude l'identité de l'intéressé. L'adresse électronique est nécessaire afin de lui envoyer par voie électronique les informations et documents qui lui sont destinés. La donnée « langue » est requise pour éviter que des informations et documents ne soient transmis à la personne concernée dans une langue qu'elle ne maîtrise pas.

Les informations auxquelles l'intéressé a accès et qui lui seront fournies / peuvent lui être fournies seront différentes selon que l'intéressé se manifeste en son nom propre ou à titre professionnel. Ceci ressortira du rôle.

Si quelqu'un sollicite l'accès à titre professionnel, il faut pouvoir contrôler que c'est à bon droit. De là vient que le numéro d'entreprise de l'institution ou de l'organisation dans laquelle travaille l'intéressé doit être communiqué, tout comme l'adresse officielle de cette institution ou organisation. Afin d'éviter que l'on ne mésuse de l'accès dont dispose une personne absente durant une longue période, par exemple par suite d'un congé de maternité, son accès (mot de passe et nom d'utilisateur) peut être suspendu (bloqué) pour la durée de son absence. Pour le bon fonctionnement de leur gestion des utilisateurs et de l'accès, il est nécessaire que les demandeurs sachent si l'accès d'une personne est actif ou non.

Il ressort de tout ceci qu'en ce qui concerne les données à caractère personnel auxquelles l'accès est demandé, la demande est conforme à l'article 4, § 1, 3° de la LVP.

C.2. Par rapport à la fréquence et à la durée de l'accès demandé.

Les demandeurs veulent obtenir un accès pour une durée indéterminée. Cette demande d'accès est formulée dans le cadre du projet de « e-government », qui n'est pas limité dans le temps. Dans cette optique, il est indiqué que l'accès soit accordé aussi longtemps que les demandeurs en ont besoin pour réaliser la gestion des utilisateurs et de l'accès.

Les demandeurs sollicitent un accès permanent. De la sorte, il disposeront des dernières données actualisées en ce qui concerne les personnes déjà enregistrées et auront d'autre part immédiatement accès aux données des personnes nouvellement enregistrées.

C.3. Par rapport au délai de conservation.

Aucune proposition concrète n'est formulée quant au délai de conservation des données. Il peut difficilement en aller autrement, puisqu'il est impossible d'estimer à l'avance pendant combien de temps l'intéressé aura recours aux services électroniques fournis par les demandeurs.

Ces derniers doivent donc veiller à ce que les données relatives à la personne concernée ne soient pas conservées plus longtemps que nécessaire pour la gestion des utilisateurs et de l'accès.

C.4. Usage interne et/ou communication à des tiers.

Les données seront exclusivement utilisées par les demandeurs et leurs sous-traitants. Quant à ces derniers, il ressort des explications procurées oralement que les requérants ont principalement en vue les tiers assurant leur appui informatique. Pour autant que cela soit nécessaire, ces données seront communiquées aux sous-traitants en vue du développement et de la maintenance des applications informatiques concernant la gestion des utilisateurs et de l'accès. Elles ne circuleront pas hors de ce groupe cible.

La commission attire l'attention sur le fait que si un des demandeurs souhaite communiquer des données à un sous-traitant, il ne peut le faire que moyennant le respect des conditions formulées à l'article 16 de la LVP.

D. SECURITE.

D.1. Généralités.

En conséquence de l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale*, toute institution de sécurité sociale est tenue, ainsi que toute institution à laquelle le réseau de la sécurité sociale est étendu, de développer une culture de sécurité et en particulier d'être attentive à la sécurité des données à caractère personnel qu'elle traite ou échange. Le service chargé de la sécurité de l'information joue un rôle important à cet égard (conseiller, encourager, contrôler, documenter). Il est dirigé par le conseiller en sécurité qui doit être désigné, en application des articles 24 et 25 de la loi du 15 janvier 1990, par toute institution de sécurité sociale et toute institution à laquelle est étendu le réseau de la sécurité sociale.

Ce conseiller rédige à l'intention du responsable de la gestion journalière de l'institution un projet de plan de sécurité de l'information, avec indication des moyens requis pour réaliser celui-ci (art.8 de l'arrêté royal du 12 août 1993).

Chaque année, un rapport relatif à la sécurité de l'information est également établi au bénéfice du responsable précité. Il comprend notamment les éléments suivants :

- un aperçu général de la situation en matière de sécurité, de l'évolution au cours de l'année écoulée et des objectifs devant encore être atteints ;
- un résumé des avis écrits transmis au responsable de la gestion journalière, avec mention de la suite qui y a été accordée ;
- un aperçu des travaux exécutés par le service chargé de la sécurité de l'information – avec le relevé de tous les incidents constatés qui étaient de nature à compromettre la sécurité de l'information de l'institution ou du réseau ;
- un relevé des campagnes menées en vue de promouvoir la sécurité ;
- une vue d'ensemble des formations suivies ou encore à suivre.

Le conseiller en sécurité de l'information veille en outre au respect des normes minimales de sécurité au sein de l'institution. Chaque année, la Banque Carrefour de la Sécurité sociale

interroge toutes les institutions quant à l'observance des normes de sécurité minimales. Les résultats de l'enquête sont communiqués au comité sectoriel de la sécurité sociale, qui prend le cas échéant les mesures nécessaires.

Dans l'exercice de sa mission, le conseiller en sécurité suit les règles reprises dans le code éthique élaboré par le groupe de travail commun « sécurité de l'information ».

Conformément à l'article 4 de l'arrêté royal du 12 août 1993, le comité sectoriel de la sécurité sociale institué au sein de la Commission de la protection de la vie privée émet un avis relativement à la désignation des conseillers en sécurité des institutions publiques de sécurité sociale. Dans ce but, le comité vérifie notamment si les connaissances de l'intéressé sont suffisantes, s'il dispose du temps nécessaire pour effectuer les tâches dévolues au conseiller en sécurité et s'il n'exerce pas d'activités incompatibles avec cette mission. L'identité du conseiller en sécurité et de ses éventuels adjoints est communiquée au comité sectoriel de la sécurité sociale aussitôt qu'il(s) a /ont été désigné(s).

De plus, le comité sectoriel de la sécurité sociale est régulièrement informé de la politique menée au sein du réseau de la sécurité sociale en matière de sécurité de l'information et peut formuler des recommandations à ce propos.

Lors de la consultation et de l'utilisation des données pour des tâches de gestion des utilisateurs et de l'accès, ainsi qu'en cas de communication électronique, les institutions de sécurité sociale et les institutions auxquelles le réseau de la sécurité sociale est étendu respecteront les normes minimales de sécurité, directives et protocoles de sécurité en vigueur en ce qui concerne l'accès au réseau de la sécurité sociale. Ces mêmes institutions signaleront aux utilisateurs que des sanctions sévères sont prévues en cas de consultation ou d'utilisation des données contraire aux clauses de l'autorisation délivrée par le comité sectoriel compétent de la Commission de la protection de la vie privée.

La liste des personnes autorisées à accéder aux données à des fins de communication sera établie et constamment actualisée. Elle sera tenue à la disposition du comité sectoriel pour l'autorité fédérale.

D.2. Personnes ayant accès aux données et liste de ces personnes.

La consultation des données de Fedict et leur utilisation dans le cadre de la gestion des utilisateurs et de l'accès sont réservées aux membres du personnel des demandeurs et de leurs sous-traitants qui seront désignés à cet effet. Il s'agit en particulier des membres du personnel qui ont besoin de ces données pour s'acquitter de leurs tâches.

POUR CES MOTIFS,

la Commission autorise les demandeurs à avoir accès, en permanence et pour une durée indéterminée, aux données suivantes du fichier d'identification électronique de Fédict :

- le numéro d'identification de la sécurité sociale (pour autant que le demandeur soit autorisé à utiliser celui-ci) ;
- le nom et le prénom ;
- le rôle (citoyen ou collaborateur) ;
- l'adresse électronique ;
- la langue ;
- le nom d'utilisateur.

Si l'intéressé est un collaborateur, il faut encore ajouter les données suivantes :

- le numéro d'entreprise de l'institution ou organisation concernée ;
- le nom de l'institution ou organisation ;
- son adresse officielle ;
- le statut (actif, bloqué ou suspendu).

La Banque Carrefour de la Sécurité sociale est tenue de tenir à la disposition de la Commission une liste reprenant l'identité de toutes les institutions de sécurité sociale, de tous les organismes intégrés dans le réseau de la sécurité sociale en vertu de l'article 18 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et des dispensateurs de droits supplémentaires visés à l'article 11bis de la loi précitée qui auront accès aux données du fichier d'identification électronique de Fedict susmentionnées. Cette liste sera actualisée chaque fois que l'accès sera accordé à un nouvel organisme.

L'administrateur, Le président,

(sé) Jo BARET (sé) Michel PARISSE